AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated in the following listing of all claims:

---

1. (Currently Amended) A method of performing point doublings in a computing system comprising:

generating a first point doubling using an initial point (x, y) comprising generating a current slope value and a current x value;

generating a second point doubling comprising generating a ~~new current x value and~~ new current slope value with at least one square operation without computing a y coordinate ~~using a multiplication step~~, and generating a new current x value with the new current slope value.

2. (Original) The method of claim 1 wherein said generating said second point doubling comprises generating a new current x value and new current slope value without using a y term.

3. (Original) The method of claim 1 wherein said generating said second point doubling comprises storing said current x value as a prior x value and storing said current slope value as a prior slope value; generating a new current x value using said prior slope value; and generating a new current slope value using said new current x value and said prior x value.

4. (Original) The method of claim 3 wherein said new current x value is generated by:

$x_1 = s^2 + s + a$

where s is said prior slope value.

5. (Original) The method of claim 3 wherein said new current slope value is generated by:

$g = (x + x_1)^2 / x_1 + (s+1)$

where x is said prior x value and x1 is said current x value.

6. (New) A method of generating an *n*th point doubling for a point (x_0, y_0) for a security value, the method comprising:

generating an initial slope with $slope_1 = x_0 + y_0/x_0$;

generating an initial x_1 with $slope_1^2+slope_1+A$, wherein A is a constant;

generating successive slopes with $slope_i = (x_{i-2}+x_{i-1})^2/x_{i-1} + (slope_{i-1} + 1)$, wherein i corresponds to succession;

generating successive x values with $x_i = (slope_i)^2 + slope_i + A$;

generating a final y value for the *n*th point doubling with $y_n = x_{n-1}^2 + (slope_n + 1)*x_n$; and

supplying the final y value and the final x value for generation of a security value.

7. (New) The method of claim 6 wherein the security value includes one or more of an encryption key and a value to determine an encryption key.

8. (New) The method of claim 7 wherein generation of the *n*th point doubling is performed with squares and reciprocals and without multiplication.

9. (New) The method of claim 6 wherein the successive slopes and the successive x values are generated without a y value.

10. (New) The method of claim 6 wherein the point (x_0, y_0) is an element of a field $F(_2m)$, wherein the x coordinate and the y coordinate are represented with *m*-bit strings.

11. (New) The method of claim 6 embodied as a computer program product, encoded on one or more machine readable media.

12. (New) A method of generating a security value comprising:

repeatedly performing reciprocals and squares to determine successive x values and successive slopes for *n* point doublings of a point (x, y), wherein the reciprocals are used to determine successive slopes and the squares and successive slopes are used to determine successive x values; and

generating y_n from x_n , x_{n-1}, and $slope_n$, wherein x_n, x_{n-1}, and $slope_n$ have been determined with one or more preceding x values and one or more preceding slopes.

13. (New) The method of claim 12 further comprising decomposing a scalar multiplication $Q = kP$ into point additions and repeated point doublings, wherein P is represented by the coordinates (x, y).

14. (New) The method of claim 13 further comprising separating k into zero windows and non-zero windows.

15. (New) The method of claim 13 further comprising looking up the point additions in a look-up table.

16. (New) The method of claim 13 wherein Q and P are security values for elliptic curve cryptography.

17. (New) The method of claim 12 wherein the successive x values are determined with $x_i = (slope_i)^2 + slope_i + A$ and the successive slopes are determined with $slope_i = (x_{i-2}+x_{i-1})^2/x_{i-1} + (slope_{i-1} + 1)$, wherein i corresponds to succession.

18. (New) The method of claim 12 wherein the y_n is generated with $y_n = x_{n-1}^2 + (slope_n + 1)*x_n$.

19. (New) The method of claim 12 embodied as a computer program product encoded on one or more machine-readable media.

20. (New) A computer program product, embodied on one or more machine-readable media, the computer program product comprising:

a first sequence of instructions to determine, for successive point doublings, successive slopes based at least in part on preceding slopes and preceding x values, and successive x values based at least in part on corresponding ones of the successive slopes and preceding x values;

a second sequence of instructions to determine a final y value with a final x value and a preceding slope, for a final point doubling, wherein the final x value and the final

y value correspond to an initial x value and an initial y value before repeated point doublings; and

a third sequence of instructions to provide the final x value and the final y value for one or more security operations.

21. (New) The computer program product of claim 20 further comprising a fourth sequence of instructions to decompose a scalar multiplication into one or more point doublings.

22. (New) The computer program product of claim 21 further comprising the fourth sequence of instructions to also decompose the scalar multiplication into point additions.

23. (New) The computer program product of claim 20 wherein the first sequence of instructions determines the successive x values in accordance with $x_i = (slope_i)^2 + slope_i + A$ and determines the successive slopes in accordance with $slope_i = (x_{i-2}+x_{i-1})^2/x_{i-1} + (slope_{i-1} + 1)$, wherein i corresponds to succession, wherein i corresponds to succession.

24. (New) The computer program product of claim 20 wherein the second sequence of instructions determines the final y value in accordance with $y_n = x_{n-1}^2 + (slope_n + 1)*x_n$, wherein n corresponds to a final succession.

25. (New) The computer program product of claim 20 wherein the first sequence of instructions determines the successive x values and the successive slopes without a y value.

26. (New) The computer program product of claim 20 wherein the first sequence of instructions determines the successive x values and the successive slopes with square operations and inverse operations, but without multiplication.

27. (New) An apparatus comprising:

memory; and

means for performing repeated point doublings with successive slopes based on slopes and x values of preceding point doublings, but without y values, and successive x values based on corresponding ones of the successive slopes.

28. (New) The apparatus of claim 27 wherein the memory hosts pre-computed point additions.

29. (New) The apparatus of claim 27 further comprising means to decompose a scalar multiplication into one or more point doublings.

30. (New) The apparatus of claim 29 further comprising means to decompose the scalar multiplication into point additions.